As empresas com baixo desempenho em cibersegurança precisam em média de mais do que o dobro do tempo daquelas bem-sucedidas nesses esforços, diz estudo da EY

O tempo de detecção e resposta a um **incidente de segurança** faz diferença para a contenção dos danos provocados às empresas, como prejuízos financeiros diretos, decorrentes muitas vezes da interrupção das operações, e comprometimento da reputação. Quanto maior esse tempo, maior também é a extensão dos danos causados. As empresas com baixo desempenho em cibersegurança levam em média 11 meses para detectar e responder a um incidente cibernético. Já aquelas mais eficazes reduzem em mais da metade para cinco meses em média. A maioria das organizações (76%) precisa de seis meses ou mais para detectar e responder a um incidente.

“Mesmo esse tempo menor não pode ser considerado bom, já que estamos falando de cinco meses para superar uma situação crítica que traz tensão e mobiliza em regime de urgência muitos recursos da empresa, como as horas dos profissionais envolvidos, que poderiam estar sendo direcionados para aquilo que se espera: o atingimento das metas de negócio”, diz Marcos Sêmola, sócio da EY para consultoria em cibersegurança. “As empresas costumam demorar para detectar o incidente. E isso é muito perigoso, pois elas nem mesmo sabem que estão sob ataque. Algumas só percebem depois do **vazamento de dados** ou da interrupção do acesso aos seus sistemas”, completa.

Os dados mencionados fazem parte do “EY 2023 Global Cybersecurity Leadership Insights Study”, que revela, ainda, que apenas um em cada cinco líderes de segurança cibernética considera seus esforços eficazes no presente e bem posicionados para o futuro. Foram entrevistados 500 líderes de segurança cibernética, incluindo 250 CISOs (Chief Information Security Officers), em oito grupos de indústrias e 25 países que abrangem as Américas (o equivalente a 50% da amostra), Ásia-Pacífico e EMEIA (Europa, Oriente Médio, Índia e África). As empresas ouvidas têm faturamento anual superior a US$ 1 bilhão. No ano passado, cada empresa sofreu em média 44 incidentes cibernéticos. Nos últimos cinco anos, houve aumento de 75% no número de ataques.

Seguras e propensas a ataques

Para chegar aos tempos médios de detecção e resposta citados, além de outros indicadores, a pesquisa dividiu as empresas em seguras, reunindo quem está fazendo o melhor trabalho, e propensas a ataques, que têm um baixo desempenho em segurança cibernética.

As seguras são rápidas na adoção da tecnologia emergente e na utilização da automação para orquestrar sua tecnologia de segurança cibernética, agilizando os processos. Elas têm estratégias específicas para gerenciar **superfícies de ataque complexas na nuvem**, no local e em terceiros. Por fim, **integram a segurança cibernética** em todos os três níveis da organização, ou seja, do C-Suite, passando pela força de trabalho em geral e chegando à própria equipe de segurança cibernética.

Mais da metade das organizações (51%) classificadas como seguras estão satisfeitas com sua **abordagem de segurança cibernética**. Porcentagem semelhante (53%) concorda que está bem posicionada para as ameaças de amanhã. Essas empresas sofreram, cada uma, em média 32 incidentes no ano passado.

Por outro lado, no universo das empresas propensas a ataques, apenas 36% dizem estar satisfeitas com sua abordagem de segurança cibernética. E somente 41% concordam que estão bem posicionadas para as ameaças de amanhã.

Das 115 organizações da América Latina, 70 são propensas a ataques e 45 são seguras, o que demonstra que há muito espaço para evolução. “É fundamental que a cibersegurança faça parte das estratégias e necessidades de todos os negócios, independentemente de sua área de atuação. Esses esforços devem ser priorizados em uma realidade de sofisticação dos ataques cibernéticos,

que têm evoluído mais rápido do que os mecanismos de defesa de muitas empresas”, finaliza Sêmola.

Fonte: FenaCap, em 25.08.2023.